No. 06-1222 Oct. 30, 2006

In the
Supreme Court of the United States

EDDIE PAUL MUNOZ; PRO SE,
- Petitioner

v.

CENTRAL TELEPHONE
COMPANY NEVADA; ET AL
-Respondents

On Petition for a Writ of Certiorari to the United States Court of Appeals for the 9th Circuit

APPENDIX Q-R-S-T
VOLUME 4

EDDIE PAUL MUNOZ : Pro Se
P.O. BOX 61344
LAS VEGAS, NEVADA 89160

APPENDIX Q

PGS A -218-226

UNITED STATES DISTRICT

COURT HEARING TRANSCRIPT

OF 1-24-2005 9: 35 AM

United States District Court
District of Nevada
Las Vegas, Nevada

EDDIE PAUL MUNOZ
Plaintiff
Vs.
SPRINT TELEPHONE COMPANY
Defendant

Las Vegas, Nevada
January 24, 2005
9:35 a.m.

ORAL ARGUMENT ON DEFANDANT'S MOTION TO DISMISS (#10)

THE HONORABLE ROBERT C. JONES PRESIDING
UNITED STATES DISTRICT COURT JUDGE

COURT RECORDER:
LILIA ABARCA de CARTER
U.S. District Court

TRASCRIPTION BY:
NW TRANSCRIPTS, LLC
Nevada Division
1027 S. Rainbow Blvd., Suite 148
Las Vegas, Nevada 89145-6232
(702) 395-2742

Proceedings recorded by electronic sound recording, transcript produced by transcription service.

APPEARANCES;
FOR THE PLAINTIFF: EDDIE PAUL MUNOZ, PRO PER
Post Office Box 61344
Las Vegas, Nevada 89160

FOR THE DEFENDANT: PATRICK J. REILLY, ESQ.
Hale, Lane, Peek Dennison, Howard & Anderson
2300 West Sahara, #800
Las Vegas, Nevada 89102

PROCEEDINGS BEGIN AT 9:35 A.M.

THE COURT: Munoz versus Sprint Telephone, please.

MR. REILLY: Good morning, Your Honor. Pat Reilly appearing on behalf of Central Telephone Company dba Sprint of Nevada.

MR. MUNOZ: Eddie Munoz, pro se.

THE COURT: Good Morning.

MR. REILLY: Good morning, Your Honor. This is Sprint's motion to dismiss the Rule 12 (b)(6) under the Rules of Civil Procedure. Mr. Martin stole my line about "it's déjà vu all over again" so I'll have to try something else. This matter goes back to 2001 and even before.

Mr. Munoz has several aspects to his business. Number one, he is a publisher. He operates a number of newspaper vending machines up and down the Strip and throughout the city except he does not distribute newspapers, he distributes publications that advertise in-call and out-call services. The other part of his business is that he operates the in-call out-call service and he has what he calls independent contractors who go out and service the in-calls and out-calls.

He has alleged since going back even before 2001 that some unknown third party has been blocking or diverting calls that would be coming into Mr. Munoz' business and sending them to another business and that he has lost –

THE COURT: Now you had an actual hearing before the public Utilities Commission?

MR. REILLY: Full evidentiary hearing.

THE COURT: It wasn't just a procedural hearing, it was an evidentiary hearing.

MR. REILLY: We had over I believe two weeks of testimony. Mr. Munoz was represented by counsel at that proceeding and the PUC issued findings of fact and conclusions of law and dismissed that complaint. Mr. Munoz had the opportunity to seek judicial review under NRS Chapter 233 (b), he –

THE COURT: And how does that statute work? Within certain time period, 30 days or something?

MR. REILLY: Within 30 days if you wish to seek judicial review of an administrative decision you must do so and that's filing a lawsuit in State District Court. If you fail to do that that becomes a final operative judgment.

Mr. Munoz failed to seek judicial review so the decision of the PUC became final and biding. That's why we have a motion for res judicata and collateral estoppel. This matter has been heard before, it's been heard on the merits, it's a final decision. It operates as a judgment effectively.

We are entitled to dismissal of this case at this point in addition to the other reasons. There's no state action by Sprint under the Section 1983 claim. There's no private cause of action under Chapter 47 of the United States Code, and also Sprint has a tariff that restricts Mr. Munoz from obtaining money damages in this case. But primarily and most certainly this matter is barred by res judicata and collateral estoppel.

THE COURT: Thank You.

MR. REILLY: Thank You.

THE COURT: Munoz.

MR. MUNOZ: Good morning, Your Honor.

THE COURT: Good Morning.

MR. MUNOZ: Your Honor, if the court would allow me to read the following statement into the record for the purpose of having it become a part of the permanent record.

The petitioner would like to have the court record reflect that I am a pro se litigant without the—without the training and expertise of a trained attorney. It should further reflect the authority of the United States Supreme Court ruling *Bounds versus Smith* should apply to these

proceedings. Due to the extent of my skills in litigation being limited to written pleadings matters such as oral arguments will limit my actions. My pro se pleadings are presently made with the help of my first cousin who is also untrained in the law.

Therefore, the petitioner would like to state as follows: the defendant's motion to dismiss has been based upon the claim by the defendants of res judicata that bars the action by the petitioners from the proceedings. However, these defendants seem to have misinterpreted what holding of the court was in these cases presented by the petitioner in his answer to the defendant's motion to dismiss. If the court would at this time examine these cases – and I'd like to read this. He is sure to find that the PUC hearing is not a judicial order, it would create that -- that would create res judicata.

In the defendant's most recent response they are down to claiming that the PUC hearing is quasi-judicial. In the first argument they were firm that the standing of PUC (sic) order had full authority of a judicial proceedings. Your petitioner has once again been left with the burden of having to interpret the rulings for the defendants. Surely he does not think that the telecommunication Act is with less authority than a PUC or state court order.

The petitioner has proof that the defendant's phone lies that were sold to the petitioner had been compromised ad remain unsecured. My claim that went before the PUC was improperly decided resulting in dismissal.

I further believe that I have a right in federal court to have the findings reviewed pursuant to the authority to the district court. Excuse me. For the standard and review under arbitrary and capricious see *Southwestern Bell versus the PUC Utilities Commission*, 28 F.2d 45 Fifth 2000.

The court in *Pacific Bell versus PacWest Telecommunication, Inc*., 325 Federal Procedures 2d, 1114 Ninth Circuit, [unintelligible] 2000 address the force of law of the PUC rulings. And I'd like to read that.

"Under the Act there has been no delegation to the state commissions of power to fill gaps in the statue through binding rule making. State commissions have been given only the power to resolve issues in arbitration and to approve or reject interconnection agreements, no to issue rulings having the force of law beyond the relationship of parties to the agreement."

THE COURT: The problem with those cases, Mr. Munoz, is as he pointed out in his reply is that they don't apply here. We're talking about an intrastate issue the PUC clearly has authority over. If it's interstate, that is from one state to another or between companies, for example, that handle traffic interstate, then the federal statute governs it preempts. But here we're talking about intrastate When I have dealings with my own telephone company intrastate, I'm under the authority of the PUC.

MR. MUNOZ: Well, at the time of the hearing and stuff it was improperly reviewed ad nobody rebutted my information. I mean there was a lot of information that I wasn't allowed to have their officers –

THE COURT: Why didn't you file a cause of action then in court within the 30-day—

MR. MUNOZ: Because at the very beginning of this I didn't want to go to the PUC because of the political magnitude of Sprint against a sole person. I waned to go into federal court but I had to exhaust my administrative remedies before I could go in the federal court.

THE COURT: That's correct, you did.

MR. MUNOZ: And at the time it was just—

THE COURT: But my question still remains, why didn't you file then a law suit within the 30 days required by statute?

MR MUNOZ: It was felonious to waste anybody's more time in that. They had – I was financially ruined at the time. I had lost my family. I had been through so many obstacles it was just unbelievable but—

THE COURT: You were represented by an attorney before the PUC?

MR. MUNOZ: Yes, and I couldn't afford to pay him anymore. There was issues where they just—I mean it was just continuing to just break my back.

THE COURT: Mr. Munoz, quite frankly that's the answer to the question. You had the opportunity. The state statute provided you a method. Your failure to exhaust in state court or in state proceedings was the fact that you failed to file a judicial proceeding either in state court or here within that 30 days. It made that decision of the PUC final. That's the problem you face.

MR. MUNOZ: Okay. Well, I would like to put in my notice for appeal to go to the Ninth Circuit.

THE COURT: Certainly.

MR. MUNOZ: And—

THE COURT: You have a time period to file a notice of appeal, sir.

I am going to grant this motion; I'll ask counsel to prepare the order. I'm granting it number one, that cause of action one and two are barred by res judicata. That is there's a prior PUC quasi-judicial ruling after a full hearing on evidence, not just a procedural ruling. They took the evidence, you were represented by counsel, you had a full opportunity to litigate that issue. You failed to file a state court action or a federal court action within 30 days prescribed by statute. Therefore, you failed to exhaust under state law.

And third and fourth, third, that you do not have a private right of action. I've reviewed the cases. There's really not much help there, but it seems that there is no private right of action under Title 47, U.S. Code, 258 and [unintelligible].

MR. MUNOZ: Finally—

THE COURT: As you've said yourself, the 1983 action was not as important to you and I think you recognize as I do that there is no state action, no under color of law action by Sprint in that proceeding. So.

MR. MUNOZ: What does a consumer do? I mean this problem continues, I still—

THE COURT: If it's intrastate, like I say, what a consumer does is you file an action with the PUC. You

litigate it. If they – if their procedures lack due process or if their ruling is unfair then you bring your lawsuit either in state or federal court within the time prescribed by statute. If it's an interstate issue then you have to – it's the state statute that governs the PUC does have authority. The federal government or court do not have authority to interfere with that.

MR. MUNOZ: And, Your Honor – I understand.

THE COURT: If I'm wrong of course you – the appellate court will correct me.

MR. MUNOZ: You know, this is a – an ongoing problem that exists for the community. I mean I'm not the only person, you know. I mean my rights were denied, I mean - - to my Fifth and Fourteenth Amendments were violated during that hearing. I wasn't able to bring officers that wanted to testify during the – with the Homeland Security issues with our, you know, Las Vegas being a number one target in the United States.

THE COURT: The answer to that, Mr. Munoz, is very simply if they made a mistake – if the PUC made a mistake in their rulings, in the way they handled the hearing, you've got to bring a lawsuit timely.

MR. MUNOZ: Okay. So I man if I file another complaint I mean back at the door again.

THE COURT: That could be.

MR. MUNOZ: Okay.

THE COURT: Okay.

MR. MUNOZ: Well, I'll see you again, sir.

THE COURT: Thank You.

MR. REILLY: Thank You, Your Honor, I'll prepare the order.

THE COURT: Thank You. Thank you and thank you for your time.

PROCEEDINGS CONCLUDED AT 9:47 A.M.

* * * * * * * * * * *

CERTIFICATION

I (WE) CERTIFY THAT TE FOREGOING IS A CORRECT TRANSCRIPT FROM THE ELECTRONIC SOUND RECORDING OF THE PROCEEDINGS IN THE ABOVE-ENTITLED MATTER.

NW TRANSCRIPTS, LLC
NEVADA DIVISION
1027 S. RAINBOW BLVD., #148
LAS VEGAS, NEVADA 89145-6232
(702) 395-2742

(s)_____
FEDERALLY CERTIFIED MANAGER/ OWNER

Kay McCrea_____
TRANSCRIBER

2/4/05_____
DATE

APPENDIX R

PGS 227-242

SPRINT TROUBLE TICKETS

SHOW PROBABLE CAUSE

PROBLEM EXISTS UP TO DATE

Intrusion Detection

High stakes= high risk

Overview

Generating revenue is never put on the back burner, and neither should your network security system. How valuable is effective network security to your company? A single access breach can cost $1.41 million according to the CSI/FBI 2004 Computer Crime and Security Survey.*

Don't let a network intrusion go unnoticed. Get a effective, managed security solution that includes network-based intrusion detection service to go hand-in hand with your firewall protection. While firewalls keep out bad network traffic. Sprint intrusion Detection Services (IDS) safeguards your network by monitoring incoming traffic and warning against unauthorized access attempts. Sprint IDS solutions can log intrusion information around the-clock, giving you the warning you need to react quickly and protect your intellectual assets.

*CSI/FBI 2004 Computer Crime and Security Survey based on 269 respondents.

http://www.sprint.com/business/products/products/intrusionDetection.jsp

11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2585415**
Problem Type: **(Hear Conversation In Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 12:00**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9937616**
Problem Type: **(Hear Conversation In Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **10/08/2004 – 17:57**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0501430**
Problem Type: **(Double Connection While Talking) Miscellaneous**
Clear Date/Time: **11/02/2004 – 15:17**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0559627**
Problem Type: **(Callers Reach Busy – No One On Line) Can't Be Called**
Clear Date/Time: **11/08/2004 – 16:07**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0965044**
Problem Type: **(Reach Recording) Miscellaneous**
Clear Date/Time: **12/14/2004 – 09:34**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **1869214**
Problem Type: **(Callers Reach Busy – No One On Line) Can't Be Called**
Clear Date/Time: **02/13/2005 -11:45**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number:**1887007**
Problem Type: **(Callers Reach Busy- No One On Line) Can't Be Called**
Clear Date/Time: **02/14/2005 – 15:17**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2585362**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 - 11:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2617191**
Problem Type: **(No Audible Ring) Can't Call**
Clear Date/Time: **04/03/2005 – 14:53**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2641994**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/05/2005 – 11:13**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2646146**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 09:15**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **2846634**
Problem Type: **(Other) Feature**
Clear Date/Time: **04/26/2005 – 13:15**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9937616**
Problem Type: **(Hear Conversation in Background/ Cannot Communicate/ With Party) Noise**
Clear Date/Time: **10/05/2004 – 17:57**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2642155**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/05/2005 – 10:05**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2646282**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 11:00**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_ce
nter/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2879169**
Problem Type: **(Other) Feature**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_ce
nter/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **3516611**
Problem Type: **(No Dial Tone) Can't Call**
Clear Date/Time: **06/07/2005 -17:52**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2585435**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 12:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2617244**
Problem Type: **(No Audible Ring) Can't Call**
Clear Date/Time: **04/03/2005 – 14:51**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2642213**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/5/2005 – 10:40**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2646236**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 09:50**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2881641**
Problem Type: **(Hear Conversation in Background/ Cannot Communicate With Party) Noise**
Clear Date/Time: **05/1/2005 – 16:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number: **2585422**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 10:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-440-6441**
Sprint Ticket Number: **2585435**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 12:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-432-2333**
Sprint Ticket Number:**2585422**
Problem Type: **(Hear Conversation in Background/Cannot Communicate With Party) Noise**
Clear Date/Time: **04/01/2005 – 10:30**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2646262**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **04/06/2005 – 10:25**

Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2585415**
Problem Type: **(Hear Conversation In Background/ Cannot Communicate With Party) Noise**
Clear Date/Time: **04/1/2005 - 12:00**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

Sprint Local Business / Work Order Detail

View Ticket History Sprint Local Business

Telephone Number: **702-431-6722**
Sprint Ticket Number: **2617222**
Problem Type: **(No Audible Ring) Can't Call**
Clear Date/Time: **04/3/2005 - 14:55**
Contact Sprint with questions about this work order.

© 2005 Sprint. All rights reserved.

https://www.sprintbmo.com/bizpark/page/service_center/small_office/view_history_detail.j... 11/23/05

APPENDIX S

PGS-A- 243-253

EMBARQ TROUBLE TICKETS

SHOW PROBABLE CAUSE

SHELL GAME

PROBLEM EXISTS UP TO DATE

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **8742128**
Problem Type: **(Other) Feature**
Clear Date/Time: **05/19/2006 – 13:57**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9448526**
Problem Type: **(No Dial Tone) Can't Call**
Clear Date/Time: **06/28/2006 – 12:10**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9466839**
Problem Type: **(No Dial Tone) Can' Call**
Clear Date/Time: **06/29/2006 – 08:45**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9478017**
Problem Type: **(Callers Reach Busy – No One On Line) Can't Be Called**
Clear Date/Time: **06/29/2006 – 16:00**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9873610**
Problem Type:
Clear Date/Time: **07/30/2006 – 15:03**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **9993389**
Problem Type: **(Hear Conversation In Background/ Cannot Communicate With Party) Noise**
Clear Date/Time: **08/08/2006 – 9:10**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **0891275**
Problem Type: **(No Dial Tone) Can't Call**
Clear Date/Time: **09/29/2006 – 10:45**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

Embarq Local Business / Work Order Detail

View Ticket History EMBARQ Local Business

Telephone Number: **702-207-6411**
Sprint Ticket Number: **5812945**
Problem Type: **(Noisy) Noise**
Clear Date/Time: **10/26/2005 – 17:37**

Contact Sprint with questions about this work order.

© Embarq Holdings Company LLC. All rights reserved.
The name EMBARQ and the jet logo are trademark of
Embarq Holdings Company LLC.

https://managebusiness.embarq.com/bizpark/page/service_
center/small_office/view_histor... 10/6/2006

EMBARQ™

Sign Off

Trouble Ticket Search

This service is only available to customers who have previously opened a ticket. If you need additional assistance, please visit Support. To review ticket status, please enter your ticket number and click Search.

Trouble Ticket Search

Look up Ticket

Ticket Number:
SEARCH
Phone Number: 702-440-6441
SEARCH

Ticket Status Info

Ticket Status: Closed

Ticket Detail Info

Ticket Number: 9466949

Ticket Created Date and Time: 06/28/2006 at 01:34 PM PST

Problem Type: (No Dial Tone) Can't Call

Embarq Committed Date & Time: 06/29/2006 at 12:30 PM PST

Customer & Service Address/Location Info

Problem Phone #: 7024406441

Address: 4372 E. BOSTON AVE
City: LAS VEGAS
State: Nevada
ZIP: 891045308

Ticket Service Charge Info

Service Charge Description: 0.00 Customer has LineGuard. No trouble isolation charge or incremental charges to repair inside wiring or jacks.

Service Charge Status: Advised

Ticket Closing Info

Closing Date & Time: 06/29/2006 at 09:04 AM PST

Contact Us: If you would like to contact Embarq regarding this ticket or would like to cancel this ticket, click on the link directory below. Please provide the reason for canceling any ticket.

Contact Embarq regarding this ticket

© 2006 Embarq Holdings Company LLC. All Rights Reserved. The name EMBARQ and the jet logo are trademarks of Embarq Holdings Company LLC.

EMBARQ™

Sign Off

Trouble Ticket Search

This service is only available to customers who have previously opened a ticket. If you need additional assistance, please visit Support. To review ticket status, please enter your ticket number and click Search.

Trouble Ticket Search

Look up Ticket

Ticket Number:
SEARCH
Phone Number: 702-432-2333
SEARCH

Ticket Status Info

Ticket Status: Closed

Ticket Detail Info

Ticket Number: 9467045

Ticket Created Date and Time: 06/28/2006 at 01:38 PM PST

Problem Type: (No Dial Tone) Can't Call

Embarq Committed Date & Time:
06/29/2006 at 12:40 PM PST

Customer & Service Address/Location Info

Problem Phone #: 7024322333

Address:	4372 E. BOSTON AVE
City:	LAS VEGAS
State:	Nevada
ZIP:	891045308

Ticket Service Charge Info

Service Charge Description: 0.00 Customer has LineGuard. No trouble isolation charge or incremental charges to repair inside wiring or jacks.

Service Charge Status: Advised

Ticket Closing Info

Closing Date & Time: 06/29/2006 at 09:04 AM PST

Contact Us: If you would like to contact Embarq regarding this ticket or would like to cancel this ticket, click on the link directory below. Please provide the reason for canceling any ticket.

Contact Embarq regarding this ticket

© 2006 Embarq Holdings Company LLC. All Rights Reserved. The name EMBARQ and the jet logo are trademarks of Embarq Holdings Company LLC.

EMBARQ™

Sign Off

Trouble Ticket Search

This service is only available to customers who have previously opened a ticket. If you need additional assistance, please visit Support. To review ticket status, please enter your ticket number and click Search.

Trouble Ticket Search

Look up Ticket

Ticket Number:
SEARCH
Phone Number: 702-431-6722
SEARCH

Ticket Status Info

Ticket Status: Closed

Ticket Detail Info

Ticket Number: 9992545

Ticket Created Date and Time: 08/07/2006 at 03:09 PM PST

Problem Type: (No Dial Tone) Can't Call

Embarq Committed Date & Time: 08/08/2006 at 02:10 PM PST

Customer & Service Address/Location Info

Problem Phone #: 7024316722

Address: 4372 E. BOSTON AVE
City: LAS VEGAS
State: Nevada
ZIP: 891045308

Ticket Service Charge Info

Service Charge Description: 0.00 Customer has LineGuard. No trouble isolation charge or incremental charges to repair inside wiring or jacks.

Service Charge Status: Advised

Ticket Closing Info

Closing Date & Time: 08/08/2006 at 10:54 AM PST

Contact Us: If you would like to contact Embarq regarding this ticket or would like to cancel this ticket, click on the link directory below. Please provide the reason for canceling any ticket.

Contact Embarq regarding this ticket

© 2006 Embarq Holdings Company LLC. All Rights Reserved. The name EMBARQ and the jet logo are trademarks of Embarq Holdings Company LLC.

APPENDIX T

PGS A-254-269

NATIONAL SECURITY ISSUE'S

CYBER WAR

SECURING SS7

TELECOMMUNICATION NETWORKS

**Proceedings of the 2001 IEEE
Workshop on Information Assurance and Security
United States Military Academy, West Point, NY, 5-6
June 2001**

Securing SS7 Telecommunications Networks

G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi*

Abstract---Signaling System 7 (SS7) defines the network architecture, configuration and message transport protocol for Public Telephone Network (PTNs). SS7 was originally designed for a closed telecommunications community, and therefore possesses limited authentication facilities. Deregulation coupled with PTN convergence with the Internet enabling attackers to perpetrate fraud, interception and interruption on a potentially massive scale.

This paper analyzes vulnerabilities in SS7 networks and presents an attack taxonomy. The architecture of a system for detecting and responding to SS7 network attacks is also described.

Keywords--- Public telephone networks, SS7 networks, vulnerabilities, critical infrastructure protection

I. INTRODUCTION

Public Telephone Networks (PTNs) are massive heterogeneous networks comprising three overlapping sub-networks: a PTN backbone, the Internet and wireless networks [4,9,13]. The PTN backbone employs signaling, transmission and operations equipment. Signaling equipment sets up and tears down calls; it includes databases and adjunct processors for number translation and call routing. Transmission equipment carries the actual telephone conversation. Operations equipment, including the operations support system (OSS), performs

management, inventory, engineering and repair functions [12].

The older in-band signaling technique combined signaling and transmission over "homerun" copper wires. But this solution was inefficient and did not support advanced PTN service [2]. The newer-and widely used – out of-band signaling separates voice transmission from the data that manage calls. Out-of-band communication between central-office switches occurs via dedicated (private and public) X.25 data networks using special protocols, most notably Signaling System 7 (SS7), to set up calls, establish billing and return busy signals [2,12].

The global standard for telecommunications, SS7 defines procedures by which PTN elements exchange information over a digital signaling network. The SS7 standard governs network architecture, configuration and message transport. The network architecture supports base communications, routing and database access across PTNs. Dedicated out-of-band SS7 networks also help prevent in-band fraud while conserving telecommunications resources.

Although SS7 reduces in-band attacks, it introduces other vulnerabilities [8,11]. The protocol was originally designed for a closed telecommunications community; therefore, it possesses limited authentication facilities. However, deregulation now requires phone companies to provide SS7 connections to any entity for a modest fee. The Internet-PTN convergence allows attackers inroads via entities with poorly secured SS7 networks. ISDN connections are also points of unauthorized entry.

Once access to a PTN is gained, an attacker can perpetrate modification, fabrication, interception on a potentially massive scale. For example, during a terrorist bombing incident, an attacker can modify entries in a call-forwarding database to re-route all phone calls to emergency services, disrupting them and possibly increasing the number of casualties.

Very few systems exist for securing SS7 networks. Secure Logix produces Telewall, a firewall for private branch exchanges (PBXs) that controls unauthorized

access [14]. Sevis Systems has developed the Intele Guard Signaling Firewall for controlling access to central office switches [15]. Apart from these efforts, published research on defending SS7 networks against attacks is virtually non-existent.

This paper focuses on the problem of securing SS7 networks. The SS7 architecture and protocol are described, and their vulnerabilities are analyzed in detail. Taxonomy of attacks on SS7 networks is presented, and the architecture of a system for systematically detecting and responding to these attacks is described.

II. SIGNALING SYSTEM 7 (SS7) NETWORK

Public Telephone Networks (PTNs) typically are composed of a PTN backbone, the Internet and wireless networks (Figure 1) [4,9]. The PTN backbone primarily uses the Signaling System 7 (SS7) protocol, the Internet employs the TCP/IP protocol suite, and wireless networks use the CDMA, TDMA and GSM protocols [5,7]. As shown in Figure 1, the PTN backbone is connected to the Internet and wireless networks via IP and wireless gateways, respectively. In addition, the PTN backbone maintains diverse connections to entities ranging from large organizations to individual users. For example, individuals and small organizations use xDSL, Dialo-Up and ISDN connections to access the PTN (or Internet) [6]. Large organizations employ analog trunks to connect PBXs (Private Branch Exchanges) to the PTN.

The SS7 network controls many PTN features, e.g., basic call setup, management, tear down, billing and returning busy signals. It also supports advanced services such as local number portability (LNP), toll-free (800/888) and toll (900) services. Enhanced call features such as call forwarding, calling party name/number display, and three-way calling are also controlled. SS7 not only facilitates these and other new services, but also provides a more efficient and secure telecommunications network.

The SS7 standard defines the signaling architecture and protocols employed for message transport. This section describes these components in detail.

A. SS7 Architecture

The SS7 architecture comprises three signaling points: service-switching points (SSPs), signal transfer points (STPs) and service control points (SCPs) (Figure 2). Each signaling point is identified by a unique point code that facilitates the routing of signaling messages. Signaling points are connected via signaling links, typically 56 or 64 kbps bi-directional X.25 data links. SSPs are the entry and exit points for SS7 networks, i.e., they strictly originate, terminate and tandem telephone calls. They are analogous to border routers on the Internet and are the primary entry points for attackers.

Figure 2 shows an SSP (1) connected to two pairs of STPs via access (A) links, the primary channels for all STPs-SSP communications. A links simultaneously support up to 9600 connections [12]. If the number of connections exceeds 9600, the SSP diverts traffic to extended (E) links (shown connecting SSP (1) to an alternative STP in Figure 2). The architecture does not demand that SSPs be deployed with E links. Therefore, some SSPs, e.g., SSP (2) in Figure 2, cannot handle large volumes of traffic. SSPs communicate by sending signaling messages over A and E links to other SSPs via STPs. They send queries to SCPs via STPs using separate links.

Figure 2 shows the four primary line types connecting SSPs to end users: analog lines, ISDN lines, X.25 data lines and leased lines. Voice trunks are analog lines directly connected to SSPs. Analog signals received by SSPs are converted to digital signaling messages to handle the call. ISDN lines represent the next stage of PTN evolution by removing analog signals from the loop [1]. These connections contain a digital (D) channel that generates digital signaling messages (resembling SS7 packets) at customer telephones, interfacing directly to

SSPs. The C channel of an ISDN connection architecturally resembles the X..25 connections used by competitive local exchange carriers (CLECs), typically small start-up companies offering services ranging from long distance to voice mail [12]. In addition, much of the Internet is connected to SSPs via leased lines. Therefore, all data passing over these lines passes through SSPs.

Once a call has been initiated by an SSP, it is routed using a matching set of STPs. All SSPs are connected to at least one mated pair of STPs. STPs are the routers of a PTN, receiving and then routing SS7 network traffic between signaling points. Messages to outside destinations must travel through dedicated STPs. STPs facilitate database access by detecting and routing queries to SCPs. They also conned call requests between SSPs. As shown in Figure 2, STPs often link to the operations support systems (OSSs), remote maintenance centers that monitor and manage PTNs. Using signaling links, OSSs connect to STPs, introducing SS7 messages throughout the PTN.

SCPs provide database access needed for advanced services. They directly connect to STPs (like SSPs). SCPs respond to queries with information necessary to process calls, accessing information sources that maintain consumer and call information, including call management service databases (CMADBs), local number portability (LNP) and line information databases (LIDBs) [12].

B. SS7 Protocol

The SS7 protocol defines the procedures for operating and communicating over SS7 networks. The protocol resembles the popular OSI model (see Figure 3). [12]. The SS7 message transfer part (MTP) Levels 1-3 correspond directly to the physical, data link and network layers of the OSI model. The user and application parts of the SS7 protocol loosely correspond to OSI Layers 4-7; they detect the connection/disconnection protocol and the remote database access protocol.

MTP Level 1 defines the electrical characteristics of signaling links and the types of interfaces used in the network, i.g., Digital Signal O (DSOA) and V.35. DSOA is a 56/64 kbps channel within a DS1 (1.544 Mbps) facility, often used in ISDN networks and T-1 trunks [12]. DSOAs are the most commonly used interfaces in the United States. V.35 interfaces also support 56/64 kbps links, but they were designed to interface analog modems with digital lines and are no longer recommended.

MTP Level 2 ensures the sequenced delivery of all SS7 messages and provides the tools necessary for reliable transport throughout the network. MTP Level 3 routes and distributes messages to the proper destinations. Using routing tables that store point codes, the routing function finds the correct destination point codes and delivers he messages. Link, routing and traffic management of netw3ork elements all occur at the network level. Link management oversees the error levels at each link and sends messages advising of a link's failed or restored status. In cooperation with link management, routing management notifies other signaling points about the failure, and only re-routes those signals that are affected by the failure. The similarities between the SS7 and OSI protocols fade at this point.

Once MTP ensures reliable signaling between adjacent nodes, SS7-specific protocols define cross network communications such as telephone call connections, disconnections and remote function control. The ISDN user part (ISUP) provides connection-oriented services in SS7 networks, setting up and tearing down circuits for voice and data between exchanges [1,12]. ISUP also offers supplementary services for the circuits carrying the transmission, e.g., sending caller information between the end points during calls. International networks employ the telephone user part (TUP) to handle call setup and teardown. TYP is compatible with ISUP, but it does not facilitate the needs of modern digital networks, especially advanced services. Consequently, ISUP is the predominant protocol while TUP is being phased out worldwide.

The signaling connection control part (SCCP) provides connectionless and connection-oriented services, although it has only been implemented for connectionless services. While MTP provides routing between adjacent nodes, SCCP performs end-to-end routing for the transaction capabilities application part (TCAP) protocol. TCAP employs SCCP connectionless service to transport non-circuit related information between signaling points. End users in the SS7 network use TCAP for peer-to-peer communication. Since TCAP allows signaling points to remotely access each other, TCAP also supports database access. In addition, SCCP enables STPs to provide global title translation, i.e., allow originating messages to only indicate general digits, not point codes. Subsequently, STPs use SCCP to transport messages to their destinations, effectively preventing outsiders from obtaining internal network point codes.

III. SS7 NETWORK VULNERABILITIES

Major SS7 network vulnerabilities, as with the Internet, arise from the number and complexity of interfaces between distinct SS7 entities. Moreover, advanced services like call forwarding have intrinsic vulnerabilities-attackers can create havoc by modifying SCPs containing forwarding destinations.

Additional vulnerabilities arise from the increasing inter-dependence and interconnectivity between SS7 networks and the Internet [4,6,9]. Large portions of the Internet use leased phone lines. Conversely, SS7 systems are networked using Internet technologies, and often, the Internet itself. Thus, SS7 vulnerabilities can affect the Internet, and Internet vulnerabilities can affect SS7 networks. Furthermore, SS7 incorporates limited authentication procedures (because it was originally designed for a closed telecommunications community). Consequently, anyone capable of generating SS7 messages and introducing them into a network can disrupt PTN services. Figure 2 identities potential entry points for attacks (Attackers 1,2, and 3)

. Users with ISDN connections can introduce digital messages into the SS7 network [1]. Attacker 1 in Figure 2 exploits this relationship by spoofing the source telephone number and introducing malicious packets onto the network. Additionally, PTN-Internet convergence gives Attacker 2 new entry points to the network. While large regional Bell operating companies (RBOCs) have significant security staff and resources, competitive local exchange carriers (CLECs) – typically small startup companies – often have limited budgets and may be relatively insecure. Thus, Attacker 2 can gain access to SSPs by compromising networked computers at a CLEC.

The Telecommunications Act of 1996 grants an SS7 network connection to any entity (including a possibly malicious one) for a modest fee (currently $10,000) [13]. Traffic on SS7 networks is therefore suspect (Attacker 3 in Figure 2).

Because STPs and SCPs use front-end computer systems, hacker exploits that seize control of netrwork operating systems pose serious threats. Local number portability (LNP), another service mandated by the 1996 Telecommunications Act, allows telephone users to switch local providers without having to change telephone numbers. LNP is another point of vulnerability. Once access is gained to SS7 networks, attackers have it easy. Virtually no systems exist for detecting and responding to attacks.

A. SS7 Attack Taxonomy

The vulnerabilities described in the previous section entitled a slew of attacks on SS7 networks. An attack taxonomy is presented on Figure 4. The targets are SSPs, STPs and SCPs. Four types of attacks are attacks are possible: modification, interception, interruption and fabrication [10].

B.SSP Attacks

SSPs constitute the SS7 network perimeter and are the gateways for attack. Most attacks exploit SS7's weak

authentication. For example, ISDN was designed to connect the edges of SS7 networks to end users, enabling ISDN users to introduce traffic directly into an SS7 network [1]. Malicious ISDN connections used by CLECs. ISDN connections, however, are available at a much lower cost (less than $100 per month).

All SS7 network elements are susceptible to packet sniffing. However, an SSP is a prime target for sniffing specific users, because each user's traffic must flow through the corresponding SSP. Attackers can also intercept services intended for a user by appending the attacker's destination to the original destination in the message.

SSPs, like all network elements, have a maximum operating capacity. Overloading an SSP-STP connection can interrupt SSP service, denying service to a segment of users. For example, one distributed denial of service (DDoS) attack introduces large numbers of initial address messages (IAMs, i.e., ISUP messages that start call setups) and direct them at a single SSP. Attackers could also intercept all traffic at a compromised signaling point, and modify IAMs to request connections with a targeted user on the same SSP. Since message sources of ISUPs can be spoofed quite easily, SSPs cannot trace the sources of such attacks.

C. STP Attacks

STPs perform routing and all messages must pass through them. Therefore, attacks that exploit routing protocols are a major concern.

SSP traffic travels directly through STPs. Thus, attackers who compromise an STP can view all traffic to and from the corresponding SSPs. A more sophisticated attack remotely compromises an STP, and then creates a transparent bogus STP that filters traffic and re-routes it to the STP. Thus, it is possible to eavesdrop on selected conversations. Modifying the destinations of SCCP (end-to-end) messages allow corresponding telephone calls (and database queries) to be re-routed at will.

Since OSSs connect to STPs, toll fraud can be perpetrated by seizing control of the OSS via the STP. Global title digits are the digits provided by the called party address. These digits do not give the point code or subsystem number, although SCCP translates the global title digits to the appropriate point code. SCCP messages with a global title (i.g., 800 numbers) must be routed through an STP, which then translates the global title to the actual point code, usually an SCP. Points codes are sensitive information, and global title translation protects the information by requiring an originating message to only provide general information that the STP can then translate to specific point codes. However, if an STP is compromised, the point codes of internal network nodes con be determined by accessing the corresponding SCPs. Another attack can modify the global title translation database maintained within the STP.

As with all routers, STPs can be overloaded with traffic, although, this is more difficult because STPs are usually deployed in redundant mated pairs. Denial of service attacks are still be possible, however, if multiple SCP databases are modified to re-route large numbers of calls to telephone numbers on a specific SSP. Additionally, an attacker compromising multiple STPs could re-route all received messages to a target STP, in effect, overloading the STP and rendering the connected SSP useless.

The OSS is susceptible to traditional computer attacks. These include viruses, worms and Trojan horses since the Oss is typically a collection of computers.

STPs and SCPs maintain local number portability (LNP) databases that hold information for routing calls. Queries of LNP databases require considerable system resources. Therefore, LNP overload is a real threat-an attacker generating massive amounts of LNP queries can shut down STPs and/or SCPs maintaining the LNP databases. Additionally, telephone numbers in LNP databases can be modified or erased.

MTP Level 3 of the SS7 protocol provides sophisticated link traffic management [11]. Message signaling units (MSUs) can notify surrounding signaling points of a node

failure, causing traffic to be re-routed around the failed node. Fabricated MSUs could render operational signaling points useless, resulting in congestion and possible crippling of the network.

D. SCP Attacks

SCP databases that store sensitive information are highly vulnerable. Consider, for example, call management services databases (CMSDBs) that process toll-free calls [12]. Toll-free numbers do not represent the actual telephone number dialed. Instead, the toll-free number is mapped to an actual telephone number and the billing information is maintained separately. The CMSDB provides routing instructions that map the call and the billing information for the call. An attacker could fraudulently change the destination number to some other number, thus re-moving all charges for calls made to destination number. Alternatively, the owner of a toll-free number could also change the billing information to void charges.

Similar modifications are possible with billing databases, LNP databases; liner information databases (LIDBs) and others. An LIDB maintains subscriber information, including billing; collect call service, calling card service and validation, and personal identification numbers (PINs). Access to this database facilitates malicious activities ranging from identity theft to toll fraud. For example, attacker could modify the billing amounts, intercept, and even modify PINs.

Many SCP attacks utilize TCAP messages that support access and modification of SCP databases. For example, an attacker could modify the subscriber account number in a TCAP message destined for an LIDB and so avoid billing. Likewise, subscribers' PINs could be obtained by generating the appropriate TCAP requests.

Voice mail databases have similar vulnerabilities. An attacker could send a TCAP message query for a certain user's password and gain full access to his/her voice mail-box.

SCP databases are also vulnerable to interruption or denial of service attacks. A compromised SCP could simply have its databases deleted, disrupting all advanced services. Additionally, a business could interrupt a competitor's toll-free number by associating it with an unrelated, even illicit, telephone number (e.g., a phone sex company.) More seriously, an attacker could modify all the destination numbers in a call-forwarding database and route them to a single number, i.g., emergency services (911), completely shutting it down.
The fabrication of TCAP messages also permits unauthorized SCP database access and modification. Such attacks can severely disrupt SS7 network services.

IV. SS7 ATTACK MANAGEMENT SYSTEM

Attack management in An SS7 network requires the coordination of diverse platforms, operating systems and applications. The subsystems and tools constituting the attack management system, currently under development, must be strategically positioned throughout the SS7 netrwork (Figure 5).

The heterogeneous, distributed architecture requires a secure communication infrastructure that provides authentication, encryption and access control mechanisms. The infrastructure employs a combination of a private (backside) network and a VPN-style public network. Secure communication will be implemented using public/private key cryptography and secure broadcasting (with capabilities).

Since SSPs represent the SS7 network perimeter, authentication modules detect attempts at spoofing and identity subversion by comparing SS7 messages with signatures of spoofing attacks.

SS7 packet sniffers, specially designed to read and interpret SS7 messages, are the primary information gatherers of the attack management system. The sniffers are positioned to passively monitor all signaling channels (Figure 5). They continuously transmit information to the other tools on the network.

SS7 firewalls are designed actively filter SS7 messages. As shown in Figure 5, they are positioned between SSPs and STPs to control traffic at all switching points. The firewalls screen traffic for attack signatures that are maintained in a special database.

SCPs interface with databases supporting advanced PTN services. Therefore, a real time fraud analyzes is located at each SCP. The analyzers examine SCP queries (TCAP messages) for suspicious patterns. For example, they check successive TCAP messages that seek to modify telephone numbers in call forwarding databases.

SCP access control modules work in conjunction with fraud analyzers. Positioned in front of SCPs to regulate entrance, the control modules determine whether or not TCAP messages destined for SCPs are "safe" based on their source data and information received from the corresponding fraud analyzer.

Each of the tools comprising the attack management system represents a systematic response to known SS7 vulnerabilities. Obviously, the tools and system will not completely secure SS7 networks. They will, however, help address many of the major problems facing modern public telephone networks.

During the fall of 1997, telephone systems in Puerto Rico were sabotaged by physically cutting lines [3]. The convergence of information and communications into a single global network makes it possible to conduct similar attacks from afar with software. Sophisticated systems are required to address a spectrum of cyber threats – ranging from emergency service disruption to coordinated strikes designed to destroy the communications infrastructure and cripple American society [16].

While substantial attention has been directed at securing computer networks, little work had focused specifically on public telephone networks (PTNs). This paper is among the first to analyze vulnerabilities in SS7 networks and present an attack taxonomy. It is hoped that this taxonomy and the system for detecting and responding to SS7 network attacks, currently under construction, will spur

efforts to develop and deploy sophisticated systems for safeguarding telecommunications networks.

ACKNOWLEDGMENTS

The research is supported by the National Institute of Justice through the Memorial Institute for the Prevention of Terrorism (MIPT), Oklahoma City, Oklahoma.

REFERENCES

[1] U. Black, ISDN and SS7: Architectures for Digital Signaling Networks, Prentice Hall, Upper Saddle River, New Jersey, 1997.

[2] J. Bosse, Signaling in Telecommunication Networks, John Wiley and Sons, New York, 1997.

[3] D. Denning, Information Warfare and Security, Addison-Wesley, Reading, Massachusetts, 1999.

[4] I. Faynberg, et al., Converged Networks and Services: Internet-working IP and the PSTN, John Wiley and Sons, New York, 2000.

[5] S. Glisic, et al., Wireless Communications: TDMAv. CDMA, Kluwer Academic Publishers, Boston, 1997.

[6] P. Kuhn, et al., Broadband Communications: Convergence of Network Technologies, Kluwer Academic Publishers, Boston, Massachusetts, 1999.

[7] Y. Lin, et al., Wireless and Mobily Network Architectured, John Wiley and Sons, New York, 2000.

[8] G. Lorenz, et al., Characterization of attacks on public telephone networks, Proceedings of the SPIE Conference on Technology on Law Enforcement, Boston, Massachusetts, November 5-8, 2000.

[9] N. Muller, IP Convergence: The Next Revolution in Telecommunications, Artech House, Norwood, Massachusetts, 1999.

[10] C. Pfleeger, Security in Computing, Prentice Hall, Upper Saddle River, New Jersey, 1997.

[11] M. Rozenblit, Security for Network Telecommunications Management, IEEE Press, Piscataway, New Jersey, 2000.

[12] T. Russell, Signaling System #7, McGraw-=Hill, New York, 2000.
[13] F. Schneider (Ed.), Trust in Cyberspace, National Academy Press, Washington, D.C., 1999.
[14] SecureLogix Corp., San Antonio, Texas (www.securelogix.com)
[15] Sevis Systems, San Antonio, Texas (www.sevis.com).
[16] The White House, Defending America's Cyberspace: National Plan for Information Systems Protection (Version 1.0), Washington, D.C., 2000.